École ESIC

Groupe AIS

Commande CLI Cisco

Said HASHEMI

Aout 2024

Table de Matières

Table des matières

Commandes de base....3
Attribution adresse IPV4....3
VLAN....3
SVI....4
STP....5
EtherChannel....5
Dynamic Routing....6
EIGRP....6
OSPF....7
FHRP, HSRP....7
Attribution IPV6....7
ACL....8
NTP....9
DNS....9
DHCP....10
SNMP....10
Syslog....10
SSH....10
FTP et TFTP....11
NAT....11
Introduction aux Architectures LAN....12
WAN....13
Revue des API....14

Commandes de base

Enable

configure terminal

enable password <mot_de_passe>

ou enable secret <secret>

Sur la console

configure terminal

line console 0

password <votre_mot_de_passe>

login

Lignes VTY

configure terminal

line vty 0 4

password <votre_mot_de_passe> login

Wr write memory

Show running-config

Show ip interface brief

Attribution adresse IPV4

interface GigabitEthernet 0/1

ip address 192.168.1.1 255.255.255.0

no shutdown

VLAN

Access Port

vlan 10

name Sales

interface GigabitEthernet 0/1

switchport mode access

switchport access vlan 10

show vlan brief

Trunk

interface GigabitEthernet 0/2

switchport mode trunk

switchport trunk encapsulation dot1q

switchport trunk allowed vlan 10,20,30 ou all

show interfaces trunk

Vlan Natif

interface GigabitEthernet 0/2

switchport trunk native vlan 99

Routeur ROAS

interface GigabitEthernet 0/0.10

encapsulation dot1Q 10

ip address 192.168.10.1 255.255.255.0

interface GigabitEthernet 0/0.20

encapsulation dot1Q 20

ip address 192.168.10.2 255.255.255.0

interface GigabitEthernet 0/0.30

encapsulation dot1Q 30

ip address 192.168.10.3 255.255.255.0

show ip route

SVI

Ip routing

Vlan 10

Name sales

interface Vlan 10

 ip address 192.168.10.1 255.255.255.0

no shutdown

interface GigabitEthernet 0/1

switchport mode access

switchport access vlan 10

ou trunk

interface GigabitEthernet 0/2

switchport mode trunk

switchport trunk encapsulation dot1q

switchport trunk allowed vlan 10,20

STP

configure terminal

spanning-tree mode stp ou rapid-pvst

spanning-tree vlan <vlan_id> priority <valeur>

interface <interface_type> <interface_number>

port fast

spanning-tree portfast

spanning-tree portfast bpduguard enable

show

show spanning-tree

show spanning-tree vlan <vlan_id>

show spanning-tree interface <interface_type> <interface_number> portfast

EtherChannel

configure terminal

interface range <interface_type> <start_number> - <end_number>

channel-group <number> mode on

trunk ou access port

switchport mode trunk

switchport mode access

PAgP

channel-group <number> mode auto

channel-group <number> mode desirable

LACP

channel-group <number> mode passive

channel-group <number> mode active

Show

show etherchannel summary

show etherchannel <number> detail

show interfaces port-channel

Dynamic Routing

RIP

configure terminal

router rip

version 2

network <réseau_ip>

passive-interface <interface_type> <interface_number>

show ip route rip

show ip protcols

EIGRP

configure terminal

router eigrp <numéro_as>

network <réseau_ip> <wildcard_mask>

show ip route eigrp

show ip eigrp neighbors

show ip protocols

interface <interface_type> <interface_number>

ip authentication mode eigrp <numéro_as> md5

ip authentication key-chain eigrp <numéro_as> <key_chain_name>

OSPF

configure terminal

router ospf <process_id>

network 192.168.10.0 0.0.0.255 area 0

network 192.168.20.0 0.0.0.255 area 0

interface GigabitEthernet 0/1

ip ospf priority 100

passive-interface GigabitEthernet 0/1

show ip route ospf

show ip ospf neighbor

show ip ospf

FHRP, HSRP

config t

interface g0/0

standby 1 ip 192.168.1.1

standby 1 priority 110

standby 1 preempt

standby 1 timers 1 3

show standby

FHRP

interface GigabitEthernet 0/1

vrrp 1 ip 192.168.1.1

vrrp 1 priority 110

vrrp 1 preempt

show vrrp

GBLP come FHRP

Attribution IPV6

Statique

Conf t

Interface g/01

ipv6 address 2001:db8:1:1::1/64

no shut

SLAAC

- Le routeur envoie des annonces RA pour le réseau 2001:db8::/64.
- Les clients génèrent automatiquement leurs adresses IPv6 via RA reçu et leur MAC adresse sans l'intervention d'un serveur DHCPv6.
- RA : Annonce du routeur combine avec MAC de l’appareil après DAD Duplicate Adresse Detection and IID Le processus de combinaison de MAC et RA.

Exemple :

interface gigabitEthernet 0/0

ipv6 address 2001:db8::/64 eui-64

ipv6 nd prefix 2001:db8::/64

ipv6 nd other-config-flag

no shutdown

ACL

Une **ACL (Access Control List)** contrôle l'accès au réseau.

Exemples :

- **ACL Standard** :

  access-list 1 permit 192.168.1.0 0.0.0.255 # Autorise 192.168.1.0/24

  access-list 1 deny 192.168.2.0 0.0.0.255 # Bloque 192.168.2.0/24

- ACL Extended :
  access-list 100 permit tcp 10.0.0.0 0.0.255.255 host 2.2.2.2 eq 443 # Autorise HTTPS
  access-list 100 deny ip any any # Bloque tout le reste
- ACL nommés : Les **ACL nommées** permettent une gestion flexible des règles.
  ip access-list extended MY_ACL
  10 permit tcp host 192.168.3.1 any eq 22
  20 permit icmp any any # Ajouter l'ICMP (ping) après SSH

  Resequencing ACL : ip access-list resequence MY_ACL 10 10

  CDP et LLDP :
  Le **CDP (Cisco Discovery Protocol)** et le **LLDP (Link Layer Discovery Protocol)** sont des protocoles de découverte de couche 2 utilisés pour échanger des informations sur les dispositifs voisins. **CDP** est propriétaire de Cisco, tandis que **LLDP** est un standard industriel utilisé dans les environnements multi-fournisseurs. Ils partagent des informations comme le nom d'hôte et l'adresse IP, mais peuvent poser des risques de sécurité. **CDP** est activé par défaut sur les dispositifs Cisco, alors que **LLDP** doit être activé manuellement. Les deux protocoles ont des commandes de configuration et de vérification similaires.

  Cdp /lldp enable
  No cdp /lldp enable
  Cdp /lldp run
  Show cdp//lldp neighbors
  Lldp transmit
  Lldp receive

NTP

Pour assurer une synchronisation précise du temps sur un réseau, le NTP (Network Time Protocol) est utilisé pour synchroniser automatiquement l'heure des dispositifs.

show clock

clock set HH:MM:SS MONTH DAY YEAR

clock timezone ZONE OFFSET

clock summer-time NAME DATE MONTHE YEAR

ntp server IP_ADDRESS

show ntp associations

show ntp status

ntp master

DNS

Le **DNS (Domain Name System)** traduit des noms de domaine comme google.com en adresses IP compréhensibles par les ordinateurs. Cela permet aux utilisateurs d'accéder à des sites web sans retenir les adresses IP. Voici les commandes clés pour gérer le DNS sur Windows et Cisco IOS :

ipconfig /all

nslookup

ipconfig /displaydns

ipconfig /flushdns

ip dns server

ip name-server IP_ADDRESS

show hosts

DHCP

Le DHCP (Dynamic Host Configuration Protocol) automatise l'attribution des paramètres réseau comme l'adresse IP, le masque de sous-réseau, et le serveur DNS, simplifiant ainsi la configuration des appareils sur un réseau sans intervention manuelle. Voici les principales commandes pour gérer le DHCP sur Windows et Cisco IOS :

ipconfig /all

ip dhcp excluded-address START_IP END_IP

CREER UNE POOL D ADRESSE:

ip dhcp pool POOL_NAME

network NETWORK_IP SUBNET_MASK

default-router GATEWAY_IP

dns-server DNS_IP

show ip dhcp binding

ip helper-address DHCP_SERVER_IP

ip address dhcp

SNMP

SNMP (Simple Network Management Protocol) est un protocole standardisé pour la gestion des réseaux, permettant aux gestionnaires de surveiller et de configurer des dispositifs réseau. Il est structuré en trois versions principales, avec SNMPv3 offrant le niveau de sécurité le plus élevé. Voici les principales commandes pour configurer SNMP sur Cisco IOS :

snmp-server community COMMUNITY_NAME RO

snmp-server community COMMUNITY_NAME RW

snmp-server host HOST_IP version VERSION COMMUNITY_NAME

snmp-server enable traps

show running-config | include snmp et show snmp

Syslog

Syslog est un protocole pour enregistrer des événements réseau, facilitant la gestion et le dépannage. Les messages peuvent être affichés dans le CLI, stockés en RAM, ou envoyés à un serveur Syslog externe.

LOGGING [IP serveur]

SSH

SSH (Secure Shell) est un protocole sécurisé pour accéder à distance à la CLI d'un appareil, offrant chiffrement et authentification. Il remplace Telnet, qui est moins sécurisé.

hostname [NomAppareil]

ip domain-name [NomDomaine]

crypto key generate rsa

enable secret [MotDePasseEnable]

username [NomUtilisateur] password [MotDePasse]

line vty 0 15

transport input ssh

login local

exec-timeout [minutes]

FTP et TFTP

- **FTP (File Transfer Protocol)** : Protocole de transfert de fichiers utilisant TCP sur les ports 20 (données) et 21 (contrôle). Il nécessite une authentification (nom d'utilisateur et mot de passe) et permet la navigation et la gestion des fichiers et répertoires.
- **TFTP (Trivial File Transfer Protocol)** : Protocole simple utilisant UDP sur le port 69. Il ne nécessite pas d'authentification et est utilisé pour transférer rapidement des fichiers sans gestion de répertoires.

ftp ip_serveur ou ftp -n ip_serveur pour authentification

ensuite les commande cmd windows pour la gestion des fichiers.

NAT

Le NAT (Network Address Translation) modifie les adresses IP pour permettre la communication entre les réseaux privés et Internet.

IP NAT INSIDE

IP NAT OUTSIDE

IP NAT INSIDE SOURCE STATIC <IP_privée> <IP_publique>

SHOW IP NAT TRANSLATIONS

SHOW IP NAT STATISTICS

CLEAR IP NAT TRANSLATION

PAT (NAT Overload)

- **Définition** : Permet à plusieurs hôtes internes de partager une seule adresse IP publique en utilisant des numéros de port uniques.

VoIP

La présentation aborde les **VLAN voix**, l'**alimentation par Ethernet (PoE)** et la **qualité de service (QoS)**.

- **Téléphones IP** : Utilisent la VoIP via Ethernet, intégrant un commutateur interne pour partager un port avec un PC. Les **VLAN voix** priorisent le trafic vocal.
- **PoE** : Fournit de l'énergie aux appareils via le même câble Ethernet, avec des fonctions de contrôle de puissance.
- **QoS** : Améliore la qualité du trafic en priorisant les appels et vidéos, avec des techniques de gestion comme **RED** et **WRED**.
- **Sécurité** : Couvre la triade CIA, les attaques courantes (DoS, spoofing) et l'**authentification multi-facteurs**.

- **Configuration Cisco** : Propose des étapes pour sécuriser un commutateur contre les attaques DHCP, incluant le filtrage MAC et l'IP Source Guard.

Configuration de DHCP Snooping

1. **Activation globale** : ip dhcp snooping
2. **Activation par VLAN** : ip dhcp snooping vlan [VLAN_ID]
3. **Configuration des ports fiables** : ip dhcp snooping trust g0/1

Introduction aux Architectures LAN

La conception des réseaux est une discipline complexe qui nécessite une compréhension approfondie des principes fondamentaux et des besoins spécifiques des clients.

Terminologies Communes

1. **Topologie en étoile** : Tous les appareils sont connectés à un dispositif central.
2. **Topologie en maillage complet** : Chaque appareil est connecté à tous les autres.
3. **Topologie en maillage partiel** : Certains appareils sont interconnectés, tandis que d'autres ne le sont pas.

Conception LAN à 2 Niveaux

- **Niveau d'accès** : Connecte les hôtes finaux (PC, imprimantes) aux commutateurs d'accès, gérant la sécurité et le marquage QoS.
- **Niveau de distribution** : Agrège les connexions des commutateurs d'accès et se connecte aux services tels qu'Internet et WAN, servant de lien entre le niveau 2 et le niveau 3.

Conception LAN à 3 Niveaux

- **Niveau d'accès** : Comme décrit précédemment.
- **Niveau de distribution** : Relie les niveaux d'accès et le niveau central.
- **Niveau central** : Concentre le trafic entre les niveaux de distribution, optimisant l'évolutivité et les performances. Ce niveau se concentre sur la vitesse sans fonctionnalités de sécurité ou de marquage QoS.

Architecture Spine-Leaf

- Structure à deux niveaux comprenant des commutateurs "spine" et "leaf". Chaque commutateur leaf est connecté à tous les commutateurs spine, tandis que les spine et leaf ne se connectent pas entre eux, équilibrant ainsi le trafic et réduisant les goulets d'étranglement.

Réseaux SOHO

- **Définition** : Réseaux pour petits bureaux ou bureaux à domicile, souvent gérés par un routeur domestique qui combine plusieurs fonctions (routeur, commutateur, pare-feu, point d'accès sans fil).

WAN

Un **WAN** (Wide Area Network) relie des réseaux locaux (LAN) sur de grandes distances, comme des bureaux dans différentes villes.

Lignes Louées

Les **lignes louées** sont des connexions privées et coûteuses entre deux sites.

Fibres Optiques

Les **fibres optiques** offrent des connexions rapides sur de longues distances.

MPLS

Le **MPLS** utilise des étiquettes pour gérer le trafic et créer des VPN.

VPN

Les **VPN** permettent des connexions sécurisées sur Internet, avec des types comme :

- **Site-à-Site** : Relie deux sites.
- **Accès Distant** : Pour des utilisateurs individuels.

Cloud et Virtualisation

1. **Virtualisation** : Permet de faire fonctionner plusieurs systèmes sur un seul serveur.
2. **Services Cloud** : Offrent des ressources via Internet (SaaS, PaaS, IaaS).
3. **Avantages du Cloud** : Réduction des coûts, flexibilité et accès facile.

Machines Virtuelles et Conteneurs

- Les **VM** isolent les systèmes d'exploitation, tandis que les **conteneurs** sont plus légers et rapides.

VRF

Le **VRF** permet de diviser un routeur pour isoler le trafic, utile dans les réseaux MPLS.

Réseaux Sans Fil

- **Normes IEEE 802.11** : Définit les LAN sans fil (Wi-Fi).
- **Défis** : Interférences, portée, confidentialité, collisions (CSMA/CA).

Problèmes

1. **Interférences** : Bandes 2,4 GHz (meilleure portée) et 5 GHz (moins d'interférences).
2. **Couverture** : Affectée par des phénomènes physiques.

Normes 802.11

- Évoluent de 802.11 (1997) à 802.11ax (Wi-Fi 6).

Types de Réseaux

- **IBSS** : Connexion directe.
- **BSS** : Via point d'accès.
- **ESS** : Réseau étendu.
- **MBSS** : Réseau maillé.

Sécurité

- **Authentification** : WEP (obsolète), EAP, WPA.
- **Chiffrement** : TKIP, CCMP, GCMP.
- **Intégrité** : Vérification des messages.

WPA

- **WPA** : TKIP.
- **WPA2** : CCMP.
- **WPA3** : Améliorations de sécurité.

Automatisation et SDN

1. **Automatisation** : Réduit erreurs et optimise la gestion.
2. **Plans Logiques** : Données, contrôle, gestion.
3. **SDN** : Centralise le contrôle pour simplifier la gestion.

Sérialisation

- **JSON** : Format lisible pour l'échange de données.
- **XML** : Langage de balisage structuré.
- **YAML** : Lisible, utilisé dans des outils d'automatisation.

Revue des API

Une **API** permet aux applications de communiquer. Dans le cadre du **SDN**, les API facilitent la communication entre le contrôleur SDN et les dispositifs réseau. Les opérations **CRUD** (Créer, Lire, Mettre à jour, Supprimer) sont gérées par des verbes HTTP :

- **POST** : Créer
- **GET** : Lire
- **PUT / PATCH** : Mettre à jour
- **DELETE** : Supprimer

Les réponses HTTP utilisent des codes d'état pour indiquer le succès ou l'échec.

Revue du SDN

Le **SDN** centralise le plan de contrôle dans un contrôleur, avec trois couches : application, contrôle, et infrastructure. Le **SD-Access** de Cisco automatise les réseaux locaux avec une architecture sous-jacente (underlay) et superposée (overlay).

DNA Center gère les réseaux SD-Access et traditionnels, simplifiant la configuration et réduisant les erreurs humaines.

Gestion des configurations

La **dérive de configuration** est causée par des modifications non suivies. Le **provisionnement de configuration** utilise des outils comme **Ansible** (sans agent), **Puppet**, et **Chef** (avec agents) pour gérer les configurations à grande échelle.

Comparaison : Ansible est plus simple, tandis que Puppet et Chef offrent des fonctionnalités avancées pour des environnements complexes.